Configure Device Discovery

Published: 2021-08-27

The ExtraHop system can discover and track devices by their MAC address (L2 Discovery) or by their IP addresses (L3 Discovery). L2 Discovery offers the advantage of tracking metrics for a device even if the IP address is changed or reassigned through a DHCP request. The system can also automatically discover VPN clients.

Before you begin
Learn how device discovery and L2 discovery works in the ExtraHop system. Changing these settings affects how metrics are associated with devices.

Note: Packet brokers can filter ARP requests. The ExtraHop system relies on ARP requests to associate L3 IP addresses with L2 MAC addresses.

Discover local devices

If you enable L3 Discovery, local devices are tracked by their IP address. The system creates an L2 parent entry for the MAC address and an L3 child entry for the IP address. Over time, if the IP address changes for a device, you might see a single entry for an L2 parent with a MAC address with multiple L3 child entries with different IP addresses.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Device Discovery**.
4. In the Local Device Discovery section, select from the following choices:
   - Select the **Enable local device discovery** checkbox to enable L3 Discovery.
   - Clear the **Enable local device discovery** checkbox to enable L2 Discovery.
5. Click **Save**.

Discover remote devices by IP address

You can configure the ExtraHop system to automatically discover devices on remote subnets by adding a range of IP addresses.

Note: If your ExtraHop system is configured for L2 Discovery and your remote devices request IP addresses through a DHCP relay agent, you can track devices by their MAC address, and you do not need to configure Remote L3 Discovery. Learn more about device discovery.

Important considerations about Remote L3 Discovery:

- L2 information, such as device MAC address and L2 traffic, is not available if the device is on a different network from the one being monitored by the ExtraHop system. This information is not forwarded by routers, and therefore is not visible to the ExtraHop system.
- Exercise caution when specifying CIDR notation. A /24 subnet prefix might result in 255 new devices discovered by the ExtraHop system. A wide /16 subnet prefix might result in 65,535 new devices discovered, which might exceed your device limit.
- If an IP address is removed from the Remote L3 Device Discovery settings, the IP address will persist in the ExtraHop system as a remote L3 device as long as there are existing active flows for that IP address or until the capture is restarted. After a restart, the device is listed as an inactive remote L3 device.

  If the same IP address is later added through the local data feed, that remote L3 device can transition to a local L3 device, but only if the capture process is restarted and the Local Device Discovery setting is enabled.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Device Discovery**.
4. In the Remote Device Discovery section, type the IP address in the IP address ranges field. You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.

   Important: Every actively communicating remote IP address that matches the CIDR block will be discovered as a single device in the ExtraHop system. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.
5. Click the green plus icon (**+**) to add the IP address. You can add another IP address or range of IP addresses by repeating steps 5-6.

   Important: The capture process must be restarted when removing IP address ranges before the changes take effect. We recommend deleting all entries before restarting the capture process. The capture process does not need to be restarted when adding IP address ranges.

Discover VPN clients

Enable the discovery of internal IP addresses that are associated with VPN client devices.

On new ExtraHop systems, VPN client discovery is enabled by default. On upgraded systems, VPN client discovery is disabled by default.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Device Discovery**.
4. In the VPN Client Discovery section, select from the following choices:
   - Select the **Enable VPN client discovery** checkbox to enable VPN client discovery.
   - Clear the **Enable VPN client discovery** checkbox to disable VPN client discovery.
5. Click **Save**.